PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2003-244127
(43)Date of publication of application : 29.08.2003

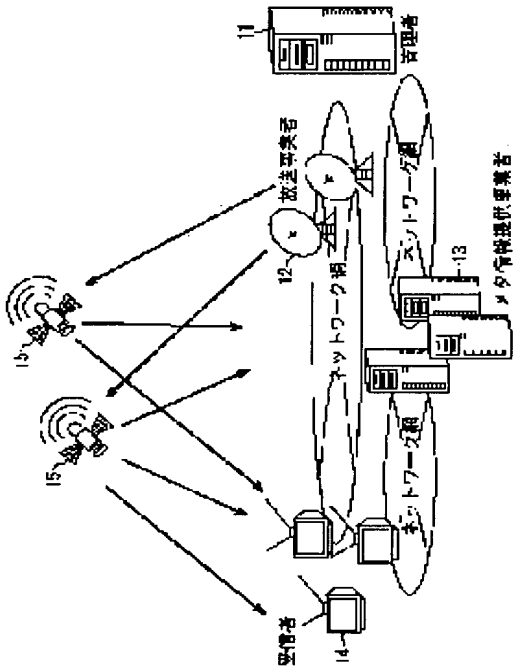
(51)Int.Cl. H04L 9/08
H04H 1/00
H04N 5/44
H04N 5/765
H04N 7/16
H04N 7/167

(21)Application number : 2002-042133
(22)Date of filing : 19.02.2002

(71)Applicant : CANON INC
(72)Inventor : TAGASHIRA NOBUHIRO

(54) DIGITAL CONTENT PROCESSING DEVICE, DIGITAL BROADCAST RECEIVER, DIGITAL CONTENT PROCESSING SYSTEM, DIGITAL BROADCAST SYSTEM, DIGITAL CONTENT PROCESSING METHOD, COMPUTER READABLE STORING MEDIUM, COMPUTER PROGRAM

(57)Abstract:
PROBLEM TO BE SOLVED: To make it possible to carry out viewing control surely for program information stored in a storage in a server-type broadcast.
SOLUTION: The digital content processing device for treating digital contents and meta-information about the digital contents includes a management means for holding first control information used for controlling the meta-information and managing the first control information by using input second control information, and a control means for controlling the usage of the digital contents or the meta-information on the basis of the first control information. Then, the viewing control at a desired time can be carried out.



LEGAL STATUS

[Date of request for examination] 11.12.2003

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)**公開特許公報**（Ａ）　(11)特許出願公開番号
特開2003－244127
（P2003－244127A）
(43)公開日　平成15年８月29日(2003.8.29)

(51)Int.Cl.[7]		識別記号	FI		テーマコード(参考)	
Ｈ０４Ｌ	9/08		Ｈ０４Ｈ	1/00	Ｆ	５Ｃ０２５
Ｈ０４Ｈ	1/00		Ｈ０４Ｎ	5/44	Ａ	５Ｃ０５３
Ｈ０４Ｎ	5/44			7/16	Ａ	５Ｃ０６４
	5/765		Ｈ０４Ｌ	9/00	６０１Ａ	５Ｊ１０４
	7/16		Ｈ０４Ｎ	7/167	Ｚ	

審査請求　未請求　請求項の数24　ＯＬ　（全 13 頁）　最終頁に続く

(21)出願番号　特願2002－42133(P2002－42133)

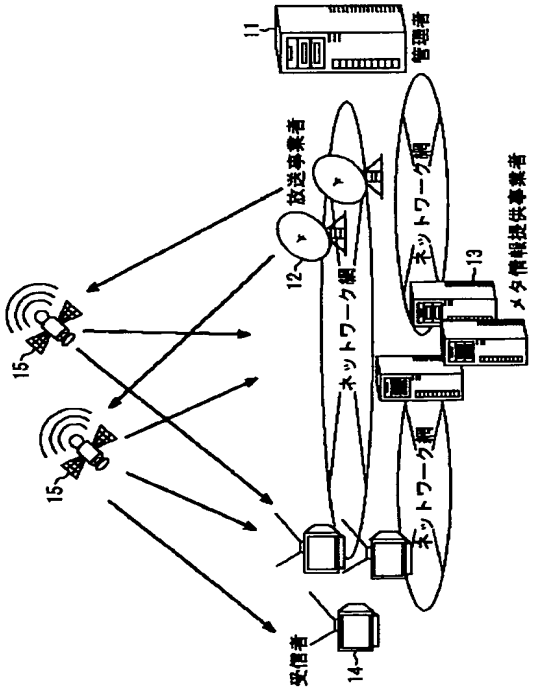
(22)出願日　平成14年２月19日(2002.2.19)

(71)出願人　000001007
キヤノン株式会社
東京都大田区下丸子３丁目30番２号
(72)発明者　田頭　信博
東京都大田区下丸子３丁目30番２号　キヤノン株式会社内
(74)代理人　100090273
弁理士　國分　孝悦

最終頁に続く

(54)【発明の名称】　デジタルコンテンツ処理装置、デジタル放送受信装置、デジタルコンテンツ処理システム、デジタル放送システム、デジタルコンテンツ処理方法、コンピュータ読み取り可能な記憶媒体及びコ

(57)【要約】
【課題】　サーバー型放送において、ストレージに蓄積された番組情報に対しても視聴制御を確実に行うことができるようにする。
【解決手段】　デジタルコンテンツ及び前記デジタルコンテンツに関するメタ情報を取り扱うデジタルコンテンツ処理装置であって、前記メタ情報を制御するための第１の制御情報を保持し、入力される第２の制御情報によって前記保持している第１の制御情報を管理する管理手段と、前記デジタルコンテンツまたは前記メタ情報の利用を前記第１の制御情報によって制御する制御手段とを設け、任意の時刻に対する視聴制御を行うことができるようにする。



1

【特許請求の範囲】

【請求項１】　デジタルコンテンツ及び前記デジタルコンテンツに関するメタ情報を取り扱うデジタルコンテンツ処理装置であって、

前記デジタルコンテンツまたは前記メタ情報を制御するための第１の制御情報を保持し、入力される第２の制御情報によって前記保持している第１の制御情報を管理する管理手段と、

前記デジタルコンテンツまたは前記メタ情報の利用を前記第１の制御情報によって制御する制御手段とを有することを特徴とするデジタルコンテンツ処理装置。

【請求項２】　前記第１の制御情報は、共通鍵暗号方式における暗号化鍵であることを特徴とする請求項１に記載のデジタルコンテンツ処理装置。

【請求項３】　前記管理手段は、前記暗号化鍵を消去することによって前記第１の制御情報を管理することを特徴とする請求項２に記載のデジタルコンテンツ処理装置。

【請求項４】　前記管理手段は、前記暗号化鍵を更新することによって前記第１の制御情報を管理することを特徴とする請求項２に記載のデジタルコンテンツ処理装置。

【請求項５】　前記第１の制御情報は、公開鍵暗号方式における復号鍵であることを特徴とする請求項１に記載のデジタルコンテンツ処理装置。

【請求項６】　前記管理手段は、前記公開鍵暗号方式における無効化リストによって前記第１の制御情報を管理することを特徴とする請求項５に記載のデジタルコンテンツ処理装置。

【請求項７】　前記第１の制御情報は、前記デジタルコンテンツまたは前記メタ情報に対応づけられていることを特徴とする請求項１～６の何れか１項に記載のデジタルコンテンツ処理装置。

【請求項８】　前記第１の制御情報は、前記デジタルコンテンツまたは前記メタ情報の配信者に対応づけられていることを特徴とする請求項１～６の何れか１項に記載のデジタルコンテンツ処理装置。

【請求項９】　前記第１の制御情報を管理する管理手段は、不正操作の困難な媒体で実現されていることを特徴とする請求項１～８の何れか１項に記載のデジタルコンテンツ処理装置。

【請求項１０】　前記請求項１～９の何れか１項に記載のデジタルコンテンツ処理装置を用いて、前記デジタルコンテンツである放送コンテンツを取り扱うことを特徴とするデジタル放送受信装置。

【請求項１１】　前記請求項１～９の何れか１項に記載のデジタルコンテンツ処理装置を有することを特徴とするデジタルコンテンツ処理システム。

【請求項１２】　前記請求項１～９の何れか１項に記載のデジタルコンテンツ処理装置を有することを特徴とするデジタル放送システム。

2

【請求項１３】　デジタルコンテンツ及び前記デジタルコンテンツに関するメタ情報を取り扱うデジタルコンテンツ処理方法であって、

前記デジタルコンテンツまたは前記メタ情報を制御するための第１の制御情報を媒体に保持し、入力される第２の制御情報によって前記保持している第１の制御情報を管理する管理工程と、

前記デジタルコンテンツまたは前記メタ情報の利用を前記第１の制御情報によって制御する制御工程とを有することを特徴とするデジタルコンテンツ処理方法。

【請求項１４】　前記第１の制御情報は、共通鍵暗号方式における暗号化鍵であることを特徴とする請求項１３に記載のデジタルコンテンツ処理方法。

【請求項１５】　前記管理工程は、前記暗号化鍵を消去することによって前記第１の制御情報を管理することを特徴とする請求項１４に記載のデジタルコンテンツ処理方法。

【請求項１６】　前記管理工程は、前記暗号化鍵を更新することによって前記第１の制御情報を管理することを特徴とする請求項１４に記載のデジタルコンテンツ処理方法。

【請求項１７】　前記第１の制御情報は、公開鍵暗号方式における復号鍵であることを特徴とする請求項１３に記載のデジタルコンテンツ処理方法。

【請求項１８】　前記管理工程は、前記公開鍵暗号方式における無効化リストによって前記第１の制御情報を管理することを特徴とする請求項１７に記載のデジタルコンテンツ処理方法。

【請求項１９】　前記第１の制御情報は、前記デジタルコンテンツまたは前記メタ情報に対応づけられていることを特徴とする請求項１３～１８の何れか１項に記載のデジタルコンテンツ処理方法。

【請求項２０】　前記第１の制御情報は、前記デジタルコンテンツまたは前記メタ情報の配信者に対応づけられていることを特徴とする請求項１３～１６の何れか１項に記載のデジタルコンテンツ処理方法。

【請求項２１】　前記第１の制御情報を保持する媒体は、不正操作の困難な媒体で実現されていることを特徴とする請求項１３～２０の何れか１項に記載のデジタルコンテンツ処理方法。

【請求項２２】前記請求項１～９の何れか１項に記載の各手段としてコンピュータを機能させるためのプログラムを記録したことを特徴とするコンピュータ読み取り可能な記憶媒体。

【請求項２３】前記請求項１３～２１の何れか１項に記載のデジタルコンテンツ処理方法をコンピュータに実行させるためのプログラムを記録したことを特徴とするコンピュータ読み取り可能な記憶媒体。

【請求項２４】前記請求項１３～２１の何れか１項に記

載のデジタルコンテンツ処理方法をコンピュータに実行させることを特徴とするコンピュータプログラム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明はデジタルコンテンツ処理装置、デジタル放送受信装置、デジタルコンテンツ処理システム、デジタル放送システム、デジタルコンテンツ処理方法、コンピュータ読み取り可能な記憶媒体及びコンピュータプログラムに関する。さらに詳しくは、蓄積機能を有するコンテンツ受信機へコンテンツを配信する場合において、蓄積されたコンテンツに対してもコンテンツの利用を制御可能なコンテンツの利用制御システムに関し、特に、蓄積機能を有する受信機であって、ネットワーク接続機能をも有する受信機向けの放送システムに用いて好適な技術に関するものである。

【０００２】

【従来の技術】昨今のデジタル化の流れにより、さまざまな分野でデジタル化が進められている。そして、放送の分野でもデジタル化が進められており、一部でデジタル放送が実現されている。

【０００３】デジタル放送では、放送番組とともに、その番組内容を記載したメタ情報などを送信することが可能であることから、大容量蓄積機能(以下、ストレージという)を有する受信機でこれらの情報を活用し、番組の自動蓄積、シーン検索、ダイジェスト視聴等など、デジタル放送のメリットを活かした新たなサービスの提案されつつある。

【０００４】国際的にも検討が進められており、TV Anytime Forumを中心に放送方式に関する技術的な検討の中で、メタ情報等に関する議論に一定の進展が図られつつある。

【０００５】また、昨今のハードディスクの大容量化に伴い、デジタル放送のコンテンツを記録するハードディスク・レコーダが既に市販されるなど、このようなサービスの実現に向けた環境が整ってきているとともに、デジタル放送においては、不正なコピーから放送コンテンツを守るための方策も必須なものとして求められている。

【０００６】なお、大容量蓄積機能を有する受信機は、インターネットや他の情報家電との接続機能など、ホームサーバーとしての機能も期待されていることから、「サーバー型受信機」と呼ばれており、またサーバー型受信機向けの放送は「サーバー型放送」と呼ぶ。

【０００７】一方、従来、有料放送方式は、テレビジョン放送や高精細度テレビジョン放送(以下、ハイビジョン放送という)に適用した限定受信方式が広く検討されてきた。

【０００８】有料方式で一般的に放送される映像信号や音声信号は、受信が許可された者以外の者により受信できないように、何らかの方法でスクランブル(撹拌)が施

され、受信が許可された者にはこのスクランブルされた信号を復元するための信号を送って受信を制御するようになっている。

【０００９】この受信を制御するための信号として送られる情報は、関連情報と呼ばれ、スクランブルを復元するための鍵(スクランブル鍵)の情報、放送される番組が各受信者の契約範囲に入っているか否かを判定するための情報、放送局から特定の受信機を強制的にオン・オフするための情報等よりなっている。

【００１０】衛星放送でテレビジョンやハイビジョンの有料放送を行う場合には、関連情報はデータチャンネルでパケットの形で伝送される。この場合、スクランブル鍵や、放送番組に関する情報(これは番組情報と呼ばれる)は、第三者に知られたり改ざんされたりしないように暗号化される。この暗号化のための鍵はワーク鍵と呼ばれ、各受信者の契約した内容を表わす契約情報とともに別途受信者に送られる。

【００１１】この関連情報は個別情報と呼ばれ、放送電波、ICカード、磁気カード等の物理媒体、電話線等で送られる。これらのうち、電波で送る場合には、必ず暗号化する必要があり、この暗号化に用いられる鍵は、マスター鍵と呼ばれ、原則的には受信者毎に異なっている。

【００１２】図１１に、このようなスクランブルを施す方式の構成例を示す。図１１において、スクランブル部１１１１、多重化部１１１２、暗号化部１１１３は放送事業者側の放送装置１１１０を示している。

【００１３】また、分離部１１２１、デスクランブル部１１２２、復号部１１２３、視聴判定部１１２４は受信者１４の受信装置１１２０側を示している。

【００１４】図１１の放送事業者側に示されるように、放送事業者は、番組情報をスクランブル鍵でスクランブルし、スクランブル鍵をワーク鍵で暗号化し、ワーク鍵と契約情報からなる個別情報をマスター鍵で暗号化し、それぞれから得られる情報を多重化して放送する。

【００１５】図１１の受信者側に示されるように、受信者１４の受信装置１１２０は、受信した情報を分離し、予め保持しているマスター鍵を用いて暗号化された個別情報を復号し、復号して得られたワーク鍵を用いて暗号化スクランブル鍵を復号し、復号して得られたスクランブル鍵と契約情報によって視聴判定を行い、許可された場合にスクランブル鍵を用いて番組情報をデスクランブルする。

【００１６】また、受信者１４側の復号部１１２３、視聴判定部１１２４はマスター鍵を安全に蓄積する必要性や、処理中に得られるワーク鍵やスクランブル鍵を受信者１４に見られないようにする必要性があり、ICカード等、外部からの不正に耐性のある媒体で実施されることが多い。

【００１７】

【発明が解決しようとする課題】従来の受信者限定方式

は、放送を想定していた。つまり、放送番組は、電波放送という通信媒体で、直接、リアルタイムで放送事業者から受信者１４へ配信されていた。これは、受信者１４による視聴制御が、電波放送受信時に、逐次視聴制御を行うことを表している。

【００１８】一方、サーバー型放送では、電波放送だけでなく、ストレージに番組情報を蓄積することを想定している。つまり、ストレージに蓄積されているコンテンツに対して、任意の時刻にアクセスすることが考えられ、任意の時刻に視聴制御を行う必要がある。しかし、従来の受信者限定方式では、任意の時刻に対する視聴制御が考慮されていなかった。

【００１９】例えば、従来の受信者限定方式において契約情報に有効な時刻情報に関する記述を含めて任意の時刻に対する視聴制御を実現した場合、契約情報の判断に利用されているICカードは正確な時刻情報を保持することができないため、時刻情報を改ざんすることで、不正視聴が可能になる恐れがある。

【００２０】これに対して、契約情報そのものを書き換えること、つまり契約情報の更新による対策が考えられる。しかし、先に説明したように、契約情報を含む個別情報は番組情報と多重化されている。

【００２１】このため、契約情報を更新することは、多重化されている情報を分離し、契約情報を抽出し、抽出した契約情報を更新し、更新した契約情報と番組情報を用いて再度多重化する必要がある。通常、多重化機能や符号化機能を持たない受信機でこれらを構成することは非常に困難である。

【００２２】さらにまた、契約情報と番組情報を分離して保持する場合が考えられる。この場合、契約情報を判断すると同時に判断する契約情報が最新であるか否かも同時に判断しなければいけないという新たな問題が生じる。

【００２３】本発明は前述の問題点にかんがみてなされたもので、サーバー型放送において、ストレージに蓄積された番組情報に対しても視聴制御を確実に行うことができるようにすることを第１の目的とする。また、すでに実現されている番組は配信方式であるBSデジタル放送を含むの既存の方式と整合性をとれるシステムを提供することを第２の目的とする。

【００２４】

【課題を解決するための手段】本発明のデジタルコンテンツ処理装置は、デジタルコンテンツ及び前記デジタルコンテンツに関するメタ情報を取り扱うデジタルコンテンツ処理装置であって、前記メタ情報を制御するための第１の制御情報を保持し、入力される第２の制御情報によって前記保持している第１の制御情報を管理する管理手段と、前記デジタルコンテンツまたは前記メタ情報の利用を前記第１の制御情報によって制御する制御手段とを有することを特徴としている。また、本発明の他の特

徴とするところは、前記第１の制御情報は、共通鍵暗号方式における暗号化鍵であることを特徴としている。また、本発明のその他の特徴とするところは、前記管理手段は、前記暗号化鍵を消去することによって前記第１の制御情報を管理することを特徴としている。また、本発明のその他の特徴とするところは、前記管理手段は、前記暗号化鍵を更新することによって前記第１の制御情報を管理することを特徴としている。また、本発明のその他の特徴とするところは、前記第１の制御情報は、公開鍵暗号方式における復号鍵であることを特徴としている。また、本発明のその他の特徴とするところは、前記管理手段は、前記公開鍵暗号方式における無効化リストによって前記第１の制御情報を管理することを特徴としている。また、本発明のその他の特徴とするところは、前記第１の制御情報は、前記デジタルコンテンツまたは前記メタ情報に対応づけられていることを特徴としている。また、本発明のその他の特徴とするところは、前記第１の制御情報は、前記デジタルコンテンツまたは前記メタ情報の配信者に対応づけられていることを特徴としている。また、本発明のその他の特徴とするところは、前記第１の制御情報を管理する管理手段は、不正操作の困難な媒体で実現されていることを特徴としている。

【００２５】本発明のデジタル放送受信装置は、前記の何れかに記載のデジタルコンテンツ処理装置を用いて、前記デジタルコンテンツである放送コンテンツを取り扱うことを特徴としている。

【００２６】本発明のデジタルコンテンツ処理システムは、前記の何れかに記載のデジタルコンテンツ処理装置を有することを特徴としている。

【００２７】本発明のデジタル放送システムは、前記の何れかに記載のデジタルコンテンツ処理装置を有することを特徴としている。

【００２８】本発明のデジタルコンテンツ処理方法は、デジタルコンテンツ及び前記デジタルコンテンツに関するメタ情報を取り扱うデジタルコンテンツ処理方法であって、前記メタ情報を制御するための第１の制御情報を媒体に保持し、入力される第２の制御情報によって前記保持している第１の制御情報を管理する管理工程と、前記デジタルコンテンツまたは前記メタ情報の利用を前記第１の制御情報によって制御する制御工程とを有することを特徴としている。また、本発明の他の特徴とするところは、前記第１の制御情報は、共通鍵暗号方式における暗号化鍵であることを特徴としている。また、本発明のその他の特徴とするところは、前記管理工程は、前記暗号化鍵を消去することによって前記第１の制御情報を管理することを特徴としている。また、本発明のその他の特徴とするところは、前記管理工程は、前記暗号化鍵を更新することによって前記第１の制御情報を管理することを特徴としている。また、本発明のその他の特徴とするところは、前記第１の制御情報は、公開鍵暗号方式

における復号鍵であることを特徴としている。また、本発明のその他の特徴とするところは、前記管理工程は、前記公開鍵暗号方式における無効化リストによって前記第１の制御情報を管理することを特徴としている。また、本発明のその他の特徴とするところは、前記第１の制御情報は、前記デジタルコンテンツまたは前記メタ情報に対応づけられていることを特徴としている。また、本発明のその他の特徴とするところは、前記第１の制御情報は、前記デジタルコンテンツまたは前記メタ情報の配信者に対応づけられていることを特徴としている。また、本発明のその他の特徴とするところは、前記第１の制御情報を保持する媒体は、不正操作の困難な媒体で実現されていることを特徴としている。

【００２９】本発明の記憶媒体は、前記に記載の各手段としてコンピュータを機能させるためのプログラムを記録したことを特徴としている。また、本発明の記憶媒体の他の特徴とするところは、前記に記載のデジタルコンテンツ処理方法をコンピュータに実行させるためのプログラムを記録したことを特徴としている。

【００３０】また、本発明のコンピュータプログラムは、前記に記載のデジタルコンテンツ処理方法をコンピュータに実行させることを特徴としている。

【００３１】

【発明の実施の形態】次に、添付図面を参照しながら本発明のデジタルコンテンツ処理装置、デジタル放送受信装置、デジタルコンテンツ処理システム、デジタル放送システム、デジタルコンテンツ処理方法、コンピュータ読み取り可能な記憶媒体及びコンピュータプログラムの実施の形態について説明する。以下に、図面を参照しながら、本発明における実施の形態を説明する。

【００３２】図１は、本発明のデジタル放送システムの実施の形態にかかるシステムの構成例を示す。実施の形態は、単一または複数の管理者と単一または複数の放送事業者と単一または複数のメタ情報提供事業者１３と複数の受信者１４から構成される。それぞれは、さまざまな通信媒体で相互接続されている。

【００３３】図１において、管理者１１は、システム全体の運用を管理する。つまり、システムで用いる鍵の発行等を管理する。図１において、放送事業者１２は、番組情報を放送によって提供するエンティティであり、一般的には放送局に相当する。ただし、実施の形態は、特に映像の放送に限った発明でなく、ラジオ放送等の音楽放送にも適応可能であるし、データ放送等の一般的なコンテンツの放送にも適応可能であることが明らかである。実施の形態では、これらの放送コンテンツを総称して番組情報と呼ぶ。

【００３４】図１において、メタ情報提供業者１３は、番組内容を記述したメタ情報を提供するエンティティである。従来の放送では、メタ情報提供業者１３は放送事業者１２と同一のエンティティであったが、サーバー型

放送を想定した場合、この限りでない。

【００３５】また、サーバー型放送では、蓄積媒体に番組情報を蓄積することを想定しており、同様にメタ情報の蓄積も想定されている。さらにまた、サーバー型受信機はネットワーク接続機能を有しているため、ネットワーク、通信衛星１５等を経由して、番組情報と独立してメタ情報を受信することも想定している。

【００３６】つまり、メタ情報の提供は、番組情報の配信時刻や通信媒体に無関係に、独立した時刻や独立した通信媒体で提供可能であり、放送事業者１２以外のエンティティから容易に行えることを示している。

【００３７】図１において、受信者１４は、番組情報を受信し、番組を視聴するエンティティである。

【００３８】放送事業者１２と他のエンティティ間は代表的には通信衛星１５を含む電波放送という通信媒体であるが、光ファイバ等のその他の通信媒体でも実現可能である。また、受信者１４とメタ情報提供事業者１３間は、放送事業者１２を経由した電波放送という一方向の通信媒体だけでなく、電話回線網、携帯電話網、ケーブルテレビ網等さまざまな双方向通信媒体も存在する。なお、放送事業者１２はメタ情報提供事業者１３になる場合もある。さらに、放送事業者１２は管理者１１になる場合もある。

【００３９】また、実施の形態において、放送事業者１２またはメタ情報提供事業者１３から受信者１４に対する、番組情報またはメタ情報の限定的な配信は、図２に示すように、従来の受信者限定方式と同様に、鍵を用いたスクランブルまたは暗号化を行うことにより実現する。

【００４０】図２は、構成を単純化するために基本的な要素だけを抽出した図を示しているが、実際に利用されている階層的な構造を持つ暗号化方式またはスクランブル方式にも対応可能である。

【００４１】受信者限定放送は、放送事業者１２またはメタ情報と受信者１４との間で鍵を共有できる場合は、番組情報またはメタ情報をデスクランブルまたは復号可能になり番組情報またはメタ情報を利用可能になるが、放送事業者１２またはメタ情報と受信者１４間で鍵を共有できない場合は、番組情報またはメタ情報をデスクランブルまたは復号不可能になり番組情報またはメタ情報を利用できないことにより実現している。

【００４２】さらにまた、実施の形態においては、サーバー型放送を想定しているので、図２に示すように受信者１４は大容量蓄積機能として、ストレージ２１を持つ。ストレージ２１には、様々な通信媒体を介して受信者１４に提供された番組情報やメタ情報が蓄積される。かつ、ストレージ２１に蓄積された番組情報やメタ情報に対しても、前述の鍵を用いた受信者限定の制御が行われる。

【００４３】図３に放送事業者１２と受信者１４の構成

の一例を示す。図３に示すように、放送事業者１２と受信者１４は通信媒体３１で接続されている。図３において、放送事業者１２は暗号化部１２１、多重化部１２２、第１の鍵管理部１２３から構成される。

【００４４】暗号化部１２１は、第１の鍵管理部１２３から入力される鍵を用いて、番組情報を暗号化する。暗号化アルゴリズムは、様々なアルゴリズムが利用可能であり、特に限定しない。

【００４５】多重化部１２２は、必要に応じて、第１の鍵管理部１２３から入力される鍵管理情報と、暗号化部１２１から入力される暗号化番組情報とを多重化する。第１の鍵管理部１２３は、図４に示すように鍵処理部４１と鍵蓄積部４２とから構成される。

【００４６】鍵蓄積部４２は複数の鍵を蓄積し、鍵処理部４１はそれらの鍵の生成や消去等の管理を行う。また、鍵処理部４１は要求に応じて蓄積されている鍵を出力し、さらに、鍵を管理するための鍵管理情報も出力する。

【００４７】鍵管理情報は、多重化部１２２へ出力し、暗号化番組情報と多重化して受信者１４に送信される場合と、通信媒体を経由して直接受信者１４へ送信される場合がある。

【００４８】図３において、受信者１４は分離部１４１、復号部１４２、第２の鍵管理部１４３から構成される。分離部１４１は、多重化された情報を、必要に応じて分離する。復号部１４２は、第２の鍵管理部１４３から入力される鍵を用いて、暗号化番組情報を復号する。復号アルゴリズムは、放送事業者１２の暗号化部１２１で用いられる暗号化アルゴリズムに対応する復号アルゴリズムである。

【００４９】第２の鍵管理部１４３は、第１の鍵管理部１２３と同様に、図４に示したように、鍵処理部４１と鍵蓄積部４２から構成される。鍵蓄積部４２は複数の鍵を蓄積し、鍵処理部４１はそれらの鍵の生成や消去等の管理を行う。また、鍵処理部４１は要求に応じて蓄積されている鍵を出力し、さらに、鍵を管理するための鍵管理情報を入力し、蓄積している鍵を管理操作する。

【００５０】第２の鍵管理部１４３は、不正な受信者１４による不正操作を困難にするために、ICカード等の不正操作の困難な耐タンパーな媒体で実現されていることが望ましい。また、耐タンパーな媒体で実現されていることで、鍵管理情報によって、自動的に鍵管理処理を実行することを可能にする。

【００５１】次に、図５を参照して、時刻推移と各エンティティの状態を説明する。まず、時刻Aにおいて、受信者１４の第２の鍵管理部１４３は鍵Key Aをだけを鍵蓄積部４２に蓄積する。鍵Key Aは契約時に予め蓄積されているものとする。また、第２の鍵管理部１４３は、ICカード等の耐タンパーな媒体に実現されており、受信者１４が自由に鍵Key Aを利用することはできない。

【００５２】時刻Bにおいて、放送事業者１２は、第１の鍵管理部１２３から鍵Key Aを出力し、鍵Key Aを用いて番組情報Pro Aを暗号化し、必要に応じて、暗号化番組情報Pro Aと鍵管理情報を多重化し、多重化した情報を放送する。

【００５３】放送を受信した受信者１４は、第１の鍵管理部１２３に鍵Key Aを蓄積しているため、暗号化番組情報Pro Aを復号可能であり、番組情報Pro Aを視聴可能である。また、受信者１４は、番組情報Pro Aをストレージ２１に蓄積する。

【００５４】時刻Cにおいても、受信者１４は、第２の鍵管理部１４３の鍵蓄積部４２に鍵Key Aを蓄積しているため、ストレージ２１に蓄積されている暗号化番組情報ProAを復号し、番組情報Pro Aを視聴可能である。

【００５５】時刻Dにおいて、放送事業者１２は、第１の鍵管理部１２３から鍵Key Bを出力し、鍵Key Bを用いて番組情報Pro Bを暗号化し、暗号化番組情報Pro Bを放送すると共に、「鍵Key Aの消去、鍵Key Bの作成」という鍵管理情報を送信する。

【００５６】送信方法は、暗号化番組情報Pro Bに多重化して送信する方法と通信媒体を経由して、鍵管理情報だけを直接受信者１４へ送信する方法があるが、特に限定しない。この鍵管理情報を受信した受信者１４の第２の鍵管理部１４３は、「鍵Key Aを消去し、鍵Key Bを生成」という処理を行う。

【００５７】第２の鍵管理部１４３は、ICカード等の対タンパーな媒体で実現されており、前述の鍵の管理処理は、鍵管理情報を受信した場合、強制的に、かつ自動的に実行される。これにより第２の鍵管理部１４３の鍵蓄積部４２には鍵Key Aだけが蓄積される。

【００５８】時刻Eにおいては、受信者１４における第２の鍵管理部１４３の鍵蓄積部４２は鍵Key Bだけしか蓄積していない。このため、鍵Key Bで暗号化された番組情報Pro Bは復号可能であり視聴可能であるが、鍵Key Aで暗号化された番組情報ProAは復号不可能であり、視聴することはできない。

【００５９】本実施の形態では、第２の鍵管理部１４３によって鍵の管理を自動的に行うことを特徴とする。特に、鍵を順次新しい鍵に更新することで、新しい鍵を持つ受信者１４だけが番組情報を視聴可能にする。また、本実施の形態では、説明を単純化するために、一つの鍵に注目して説明したが、各鍵管理部１２３，１４３は、同時に複数の鍵を管理することも可能である。

【００６０】つまり、図１０に示すように、鍵Key AとニュースA、鍵Key BとニュースB等、複数の鍵を利用し、個々の鍵を個々のコンテンツまたは個々のメタ情報毎に対応させることも可能である。コンテンツ毎に鍵を対応づけた場合、コンテンツ毎の視聴制御を可能にし、メタ情報毎に鍵を対応づけた場合、メタ情報毎の利用制御を可能にする。

11

【００６１】また、本実施の形態では、鍵を利用して暗号化番組情報または暗号化メタ情報を生成するエンティティと鍵を管理し鍵管理情報を生成するエンティティが同じ場合を説明したが、それぞれが異なるエンティティである場合も考えられる。図６に構成を示す。

【００６２】図６は、放送事業者１２とメタ情報提供事業者１３と受信者１４から構成される。放送事業者１２、メタ情報提供事業者１３、受信者１４ともに鍵を利用するが、放送事業者１２だけが鍵管理情報を生成する。

【００６３】放送事業者１２と受信者１４は前述と同様である。図６に示すメタ情報提供事業者１３は、メタ情報を提供するエンティティであって、第２の暗号化部１３１と第３の鍵管理部１３２から構成される。

【００６４】第３の鍵管理部１３２は、鍵を管理し、必要に応じて鍵を出力し、第２の暗号化部１３１は、第３の鍵管理部１３２から入力される鍵を用いて、メタ情報を暗号化し、受信者１４へ送信する。第３の鍵管理部１３２は、ICカード等、耐タンパーな媒体で実現されているものとする。

【００６５】図６では、メタ情報に関して、鍵を管理するエンティティである放送事業者１２と暗号化メタ情報を送信するエンティティが異なる。つまり、放送事業者１２は鍵を管理することにより、特定の鍵を保持するメタ情報提供事業者１３から提供されるメタ情報の利用制御を可能にする。

【００６６】特に、複数の鍵を利用し、鍵とメタ情報提供事業者１３を対応づけることにより、特定のメタ情報提供事業者１３から提供されるメタ情報の利用制御を可能にし、つまりはメタ情報提供事業者１３の有効性を制御可能にする。

【００６７】さらにまた、メタ情報提供事業者１３や放送事業者１２と鍵を対応づける方法とコンテンツまたはメタ情報と鍵を対応づける方法を組み合わせた方法も考えられるが、前述の方法を単純に組み合わせれば実現可能なので、詳細の説明は省略する。

【００６８】図７に、従来の受信者限定方式に適応させた場合の構成図を示す。図７において、放送事業者１２の放送装置７０は、スクランブル部７１、多重化部７２、第１の暗号化部７３、第２の暗号化部７４、第１の鍵管理部７５から構成される。

【００６９】第１の鍵管理部７５は、鍵を管理し、第２の暗号化部７４へ鍵を出力する。また必要に応じて、鍵管理情報を多重化部７２へ出力する。

【００７０】第２の暗号化部７４は、第１の鍵管理部７５から入力される鍵を用いて、ワーク鍵と契約情報を暗号化する。第１の暗号化部７３は、ワーク鍵を用いて、スクランブル鍵を暗号化する。スクランブル部７１は、スクランブル鍵を用いて、番組情報をスクランブルする。多重化部７２は、スクランブルされた番組情報と暗

12

号化スクランブル鍵と暗号化ワーク鍵と暗号化契約情報と必要に応じて鍵管理情報を多重化する。

【００７１】図７において、受信者１４の受信装置８０は、分離部８１、デスクランブル部８２、第１の復号部８３、第２の復号部８４、視聴判定部８５、第２の鍵管理部８６から構成される。

【００７２】第２の鍵管理部８６は、鍵を管理し、第２の復号部８４へ鍵を出力する。また、鍵管理情報を入力した場合は、入力した鍵管理情報に応じて鍵を管理する。分離部８１は、放送装置７０側の多重化部７２において行われた処理に対応する処理を行う手段であって、多重化情報を入力して分離する。第２の復号部８４は、第２の鍵管理部８６から入力した鍵を用いて、分離部８１から入力した暗号化ワーク鍵と暗号化契約情報を復号する。

【００７３】第１の復号部８３は、第２の復号部８４から入力したワーク鍵を用いて、分離部８１から入力した暗号化スクランブル鍵を復号する。視聴判定部８５は、第２の復号部８４から契約情報を入力し、かつ第１の復号部８３からスクランブル鍵を入力し、視聴の許可、または不許可を判定し、スクランブル鍵を出力する。

【００７４】デスクランブル部８２は、視聴判定部８５から入力したスクランブル鍵を用いて、スクランブルされた番組情報をデスクランブルする。

【００７５】本実施の形態では、鍵を自動的に更新することで、受信者１４のストレージに番組情報と契約情報が組で蓄積されている場合でも、鍵を無効化することで視聴制御を可能にする。特に、新しい番組の配信と同時に、鍵の制御情報を送信することで、鍵更新の自動化も実現している。

【００７６】なお、本実施の形態では、番組情報を対象に暗号化またはスクランブル処理を実現しているが、メタ情報に対しても同様に対応可能であることは明らかである。

【００７７】次に、鍵管理部に関して他の実施の形態を説明する。前述の実施の形態では、鍵管理部は、ICカード等の耐タンパーな媒体で実現されており、鍵の蓄積や鍵管理の処理は自動的に行われているという前提で述べた。つまり、鍵の保持や鍵管理の処理は安全であるという前提である。

【００７８】しかし、耐タンパーな媒体の安全性は完全でなく、他の手法により安全性を補完する必要も生じる。そこで、暗号技術を用い、鍵管理部に関して、共通鍵暗号方式をベースとした方法と公開鍵暗号方式をベースとした方式を用いることにより、安全性を向上する方式を説明する。

【００７９】さらに鍵管理情報の配信に関し、放送等の不特定多数の受信者１４向けの通信媒体を用いても、安全に、特定の受信者１４だけに鍵管理情報を提供可能な方式を説明する。

【００８０】図８は、共通鍵暗号方式をベースとした鍵管理部の構成例を示す。まず、共通鍵暗号方式に関して述べる。共通鍵暗号方式とは、共通の情報を鍵とし、鍵を送信者と受信者とで秘密に共有し、それぞれ送信者側と受信者側でこの鍵を用いてメッセージを変換する方式である。秘密に同じ鍵を共有することから、秘密鍵暗号方式、対称鍵暗号方式、慣用暗号方式とも呼ばれる。共通鍵暗号方式としては、DES暗号(Data Encryption Standard)やMISTY暗号、AES(Advanced EncryptionStandard)等が知られている。

【００８１】図８において、第１の鍵管理部８１０は、第１の鍵選択部８１１、第１の鍵処理部８１２、第１の鍵蓄積部８１３から構成されている。

【００８２】また、第２の鍵管理部８２０は、第２の鍵選択部８２１、第２の鍵処理部８２２、第２の鍵蓄積部８２３から構成される。

【００８３】図８に示す第１の鍵蓄積部８１３は、複数の鍵を蓄積する。複数の鍵は、固定鍵とそれ以外に分類される。また、第１の鍵選択部８１１は、暗号化部の要求に応じて、第１の鍵蓄積部８１３に蓄積されている複数の鍵から暗号化処理に用いる鍵を選択し、選択した鍵を出力する。

【００８４】また、第１の鍵処理部８１２は、第１の鍵蓄積部８１３に蓄積されている鍵を管理する。また、受信者の鍵を管理するための鍵管理情報を生成し、出力する。鍵を管理するとは、鍵の新たな生成や蓄積されている鍵の消去である。つまり、コンテンツやメタ情報毎に利用制御を行う場合は、新たなコンテンツを生成する毎に鍵を生成し、生成した鍵を用いてコンテンツやメタ情報を暗号化やスクランブルする。

【００８５】また、鍵管理情報は、第２の鍵蓄積部８２３に対して、新たな鍵の生成や蓄積されている鍵の消去を実現するための情報であり、新規鍵情報を含む鍵の生成を実現する命令や消去動作を実現するための命令から構成される。

【００８６】つまり、コンテンツやメタ情報を新たに配信する場合は、対応する新たな鍵を含む、鍵を追加するための命令から構成され、コンテンツやメタ情報の利用を禁止する場合は、対応する鍵の消去を実現する命令から構成される。さらにまた、必要に応じて、固定鍵を用いて鍵管理情報を暗号化する。

【００８７】図８に示す第２の鍵蓄積部８２３は、複数の鍵を蓄積する。複数の鍵は固定鍵とそれ以外に分類される。第２の鍵選択部８２１は、復号部１４２の要求に応じて、第２の鍵蓄積部８２３に蓄積されている複数の鍵から復号処理に用いる鍵を選択し、選択した鍵を出力する。

【００８８】また、第２の鍵処理部８２２は、第２の鍵蓄積部８２３に蓄積されている鍵を管理する。また、受信した鍵管理情報に従って鍵を生成したり、鍵を消去したりする。さらにまた、受信した鍵管理情報が暗号化されている場合は、固定鍵を用いて復号する。

【００８９】つまり、コンテンツやメタ情報毎に利用制御を行う場合は、新たなコンテンツやメタ情報毎に、新たな鍵を含む秘密鍵生成の命令を受信し、第２の蓄積部へ新たな鍵を生成し、蓄積し、コンテンツやメタ情報の利用を禁止する毎に、対応する鍵の消去を実現するための命令を受信し、第２の蓄積部から対応する鍵を消去する。

【００９０】共通鍵暗号方式をベースとした鍵管理部は、鍵管理情報が番組情報に多重化され、不特定多数の受信者に鍵管理情報が送信されてしまう場合でも、固定鍵で暗号化することにより安全に特定のユーザに送信可能になる。これにより、他の受信者１４に送信している新規の鍵を盗聴し、新規鍵として追加するといった不正ができなくなる。

【００９１】図９は、公開鍵暗号方式をベースとした鍵管理部の構成例を示す。まず、公開鍵暗号方式に関して述べる。公開鍵暗号方式は、暗号化する鍵と復号する鍵が異なり、片方を公開することができる暗号方式である。公開する鍵を公開鍵、他方を秘密鍵と呼び、秘密鍵は秘密に保持する。

【００９２】公開鍵と秘密鍵は１対１に対応し、公開鍵で変換したメッセージはそれに対応する秘密鍵でだけ復号可能である。さらに、公開鍵から秘密鍵は分からないように設計されている。また公開鍵暗号方式による暗号化と復号のそれぞれの処理を逆に行うことによりメッセージの署名者を特定するデジタル署名が実現できる。

【００９３】つまり、秘密鍵を所有する特定の署名者は秘密鍵でメッセージを変換して署名を生成し、公開鍵を所有可能な不特定多数の署名検証者は公開鍵で検証を行う。公開鍵暗号方式としては、RSA暗号やElGamal暗号等が知られている。

【００９４】公開鍵暗号方式を利用したシステムは、認証機関(以下、CAという)と証明書と証明書失効リスト(以下、CRLという)を利用した公開鍵インフラストラクチャ(以下、PKIという)のもとで利用されることが多い。CAによって作成された利用者の公開鍵に対する証明書と公開鍵を共に用いることにより、公開鍵の正当性を保証する。また、証明書の検証過程において、CRLを参照することにより、その証明書が取り消されていないかどうかの検査を可能にする。

【００９５】図９において、放送事業者１２がCAの機能を実現しており、第１の鍵管理部９１０は、第１の鍵選択部９１１、第１の鍵処理部９１２、第１の鍵蓄積部９１３から構成されている。

【００９６】また、第２の鍵管理部９２０は、第２の鍵選択部９２１、第２の鍵処理部９２２、第２の鍵蓄積部９２３から構成される。

【００９７】図９に示す第１の鍵蓄積部９１３は、放送

事業者に対応する秘密鍵と複数の公開鍵とCRLを蓄積する。公開鍵は放送事業者やメタ情報提供事業者や受信者に対応づけされている。また、CRLはCAによって管理されている。

【００９８】図９に示す第１の鍵選択部９１１は、暗号化部の要求に応じて、第１の鍵蓄積部９１３に蓄積されている複数の公開鍵から暗号化処理に用いる公開鍵を選択し、選択した公開鍵を出力する。

【００９９】また、第１の鍵処理部９１２は、第１の鍵蓄積部９１３に蓄積されている鍵とCRLを管理する。また、受信者の鍵とCRLを管理するための鍵管理情報を生成し、出力する。鍵管理情報は、第２の鍵蓄積部９２３に蓄積されている鍵の消去や新規鍵の追加やCRLの更新を実現するための情報であり、消去動作を実現するための命令や新規鍵情報やCRLの更新情報から構成される。また、必要に応じて、公開鍵を用いて鍵管理情報を暗号化し、秘密鍵を用いて鍵管理情報に対するデジタル署名を生成する。

【０１００】図９に示す第２の鍵蓄積部９２３は、受信者１４に対応する秘密鍵と複数の公開鍵とCRLとを蓄積する。また、第２の鍵選択部９２１は、復号部１４２の要求に応じて、第２の鍵蓄積部９２３に蓄積されている秘密鍵を出力する。

【０１０１】また、第２の鍵選択部９２１は、復号部１４２の要求に応じて、第２の鍵蓄積部９２３に蓄積されている秘密鍵を、CRLによる有効性の確認が行われた場合に出力する。さらに、第２の鍵処理部９２２は、第２の鍵蓄積部９２３に蓄積されている秘密鍵とCRLを管理する。また、受信した鍵管理情報に従って、秘密鍵を生成したり、秘密鍵を消去したり、CRLの更新する。

【０１０２】特に、受信した鍵管理情報が暗号化されている場合は、秘密鍵を用いて復号し、デジタル署名を有する場合は、CRLによる公開鍵の有効性とデジタル署名の有効性を検証し、有効である場合に鍵管理の処理を行う。

【０１０３】公開鍵暗号方式をベースとした鍵管理部は、共通鍵暗号方式をベースとした鍵管理部と同様に、鍵管理情報が番組情報に多重化され、不特定多数の受信者に鍵管理情報が送信されてしまう場合でも、秘密鍵で暗号化することにより安全に特定のユーザに送信可能になる。

【０１０４】また、CRLをベースとした鍵の有効性の検査も同時に実現可能であり、共通鍵暗号方式ベースの鍵管理方式より、簡便な鍵管理を実現する。

【０１０５】（本発明の他の実施の形態）本発明は複数の機器から構成されるシステムに適用しても１つの機器からなる装置に適用しても良い。

【０１０６】また、前述した実施の形態の機能を実現するように各種のデバイスを動作させるように、前記各種デバイスと接続された装置あるいはシステム内のコンピュータに対し、記憶媒体から、またはインターネット等の伝送媒体を介して前記実施の形態の機能を実現するためのソフトウェアのプログラムコードを供給し、そのシステムあるいは装置のコンピュータ（ＣＰＵあるいはＭＰＵ）に格納されたプログラムに従って前記各種デバイスを動作させることによって実施したものも、本発明の範疇に含まれる。

【０１０７】また、この場合、前記ソフトウェアのプログラムコード自体が前述した実施の形態の機能を実現することになり、そのプログラムコード自体、およびそのプログラムコードをコンピュータに供給するための手段、例えばかかるプログラムコードを格納した記憶媒体は本発明を構成する。かかるプログラムコードを記憶する記憶媒体としては、例えばフレキシブルディスク、ハードディスク、光ディスク、光磁気ディスク、ＣＤ－ＲＯＭ、磁気テープ、不揮発性のメモリカード、ＲＯＭ等を用いることができる。

【０１０８】また、コンピュータが供給されたプログラムコードを実行することにより、前述の実施の形態で説明した機能が実現されるだけでなく、そのプログラムコードがコンピュータにおいて稼働しているＯＳ（オペレーティングシステム）あるいは他のアプリケーションソフト等の共同して前述の実施の形態で示した機能が実現される場合にもかかるプログラムコードは本発明の実施の形態に含まれることは言うまでもない。

【０１０９】さらに、供給されたプログラムコードがコンピュータの機能拡張ボードやコンピュータに接続された機能拡張ユニットに備わるメモリに格納された後、そのプログラムコードの指示に基づいてその機能拡張ボードや機能拡張ユニットに備わるＣＰＵ等が実際の処理の一部または全部を行い、その処理によって前述した実施の形態の機能が実現される場合にも本発明に含まれる。

【０１１０】

【発明の効果】以上説明してきたように、本発明によれば、前述した問題を解決することができ、サーバー型放送においてストレージに蓄積された番組情報またはメタ情報に対しても、視聴制御を確実に行うことが可能なディジタルシステムを提供することができる。

【０１１１】また、本発明の他の特徴によれば、すでに実現されている番組は配信方式であるBSデジタル放送を含む既存の方式と整合性をとれるシステムを提供することができる。

【図面の簡単な説明】

【図１】本発明の実施の形態を示し、デジタル放送システムの概要を示した構成図である。

【図２】本発明の実施の形態のおける限定受信システムの基本構成を示した構成図である。

【図３】本実施の形態のおけるデジタル放送システムの概略を示す構成図である。

【図４】本実施の形態における鍵管理部の構成例を示す

17　　18

図である。

【図５】本実施の形態における放送事業者と受信者に関する時刻に対する状態を示した図である。

【図６】本発明の第２の実施の形態を示し、デジタル放送システムの概略構成を示す図である。

【図７】本発明を受信者限定方式に適応した実施の形態を示す構成図である。

【図８】本実施の形態の鍵管理部の第２の構成例を示す図である。

【図９】本実施の形態の鍵管理部の第３の構成例を示す図である。

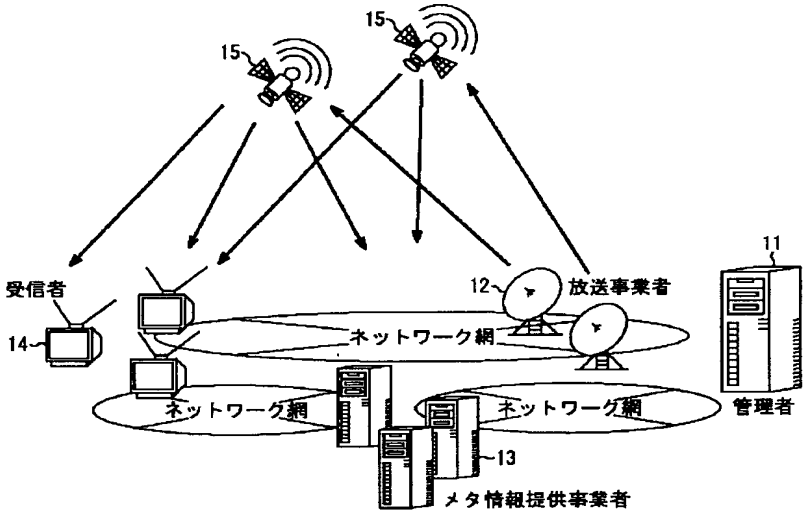
【図１０】本実施の形態のおける鍵とコンテンツの対応を示す図である。

【図１１】従来の受信者限定方法の構成を示した構成図である。

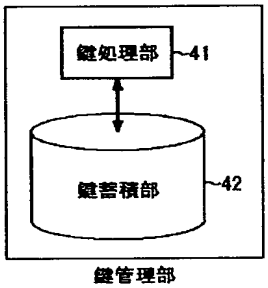
【符号の説明】

１１　管理者
１２　放送事業者
１３　メタ情報提供業者
１４　受信者
２１　ストレージ
３１　通信媒体
１２１　暗号化部
１２２　多重化部
１２３　第１の鍵管理部
１４１　分離部
１４２　復号部
１４３　第２の鍵管理部

【図１】



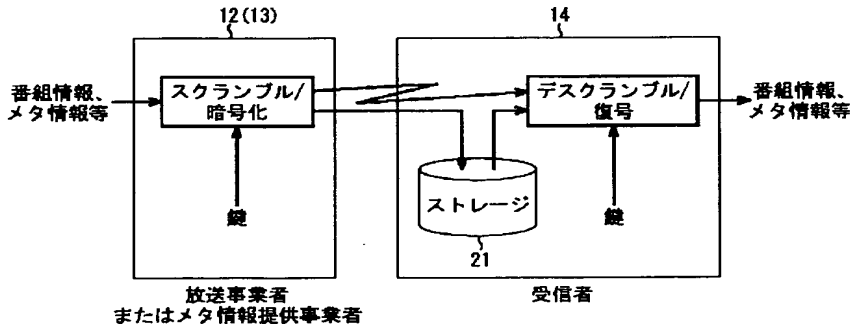
【図４】



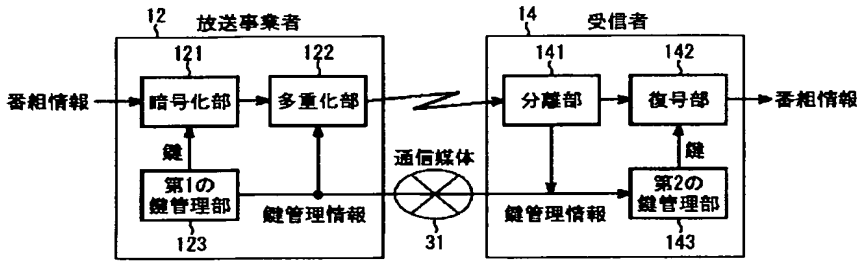
【図１０】

鍵	番組情報
KeyA	ニュースA
KeyB	ニュースB
KeyC	ドラマA
KeyD	スポーツA

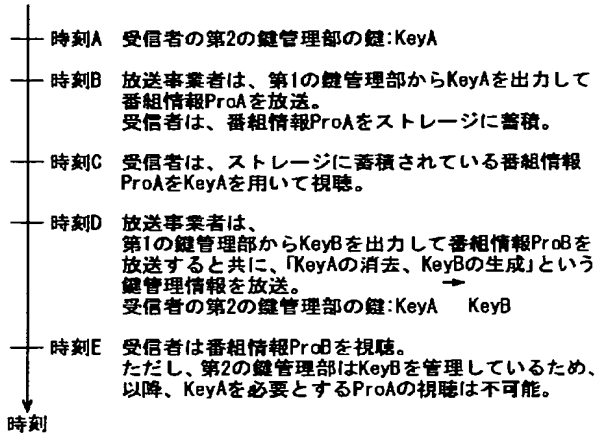
【図２】



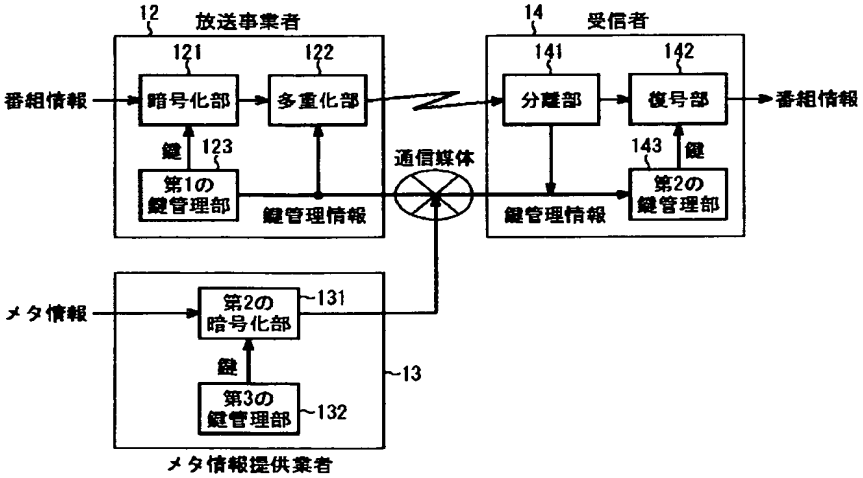
【図３】


12
放送事業者
121
122
番組情報
暗号化部
多重化部
鍵
第1の
鍵管理部
123
鍵管理情報
通信媒体
31
14
受信者
141
142
分離部
復号部
番組情報
鍵
第2の
鍵管理部
143
鍵管理情報

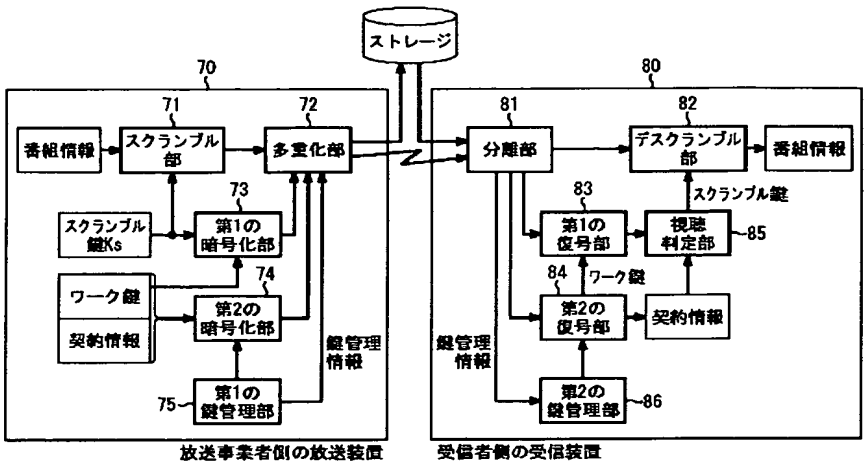
【図５】


時刻A　受信者の第2の鍵管理部の鍵:KeyA
時刻B　放送事業者は、第1の鍵管理部からKeyAを出力して
番組情報ProAを放送。
受信者は、番組情報ProAをストレージに蓄積。
時刻C　受信者は、ストレージに蓄積されている番組情報
ProAをKeyAを用いて視聴。
時刻D　放送事業者は、
第1の鍵管理部からKeyBを出力して番組情報ProBを
放送すると共に、「KeyAの消去、KeyBの生成」という
鍵管理情報を放送。
受信者の第2の鍵管理部の鍵:KeyA　KeyB
時刻E　受信者は番組情報ProBを視聴。
ただし、第2の鍵管理部はKeyBを管理しているため、
以降、KeyAを必要とするProAの視聴は不可能。
時刻

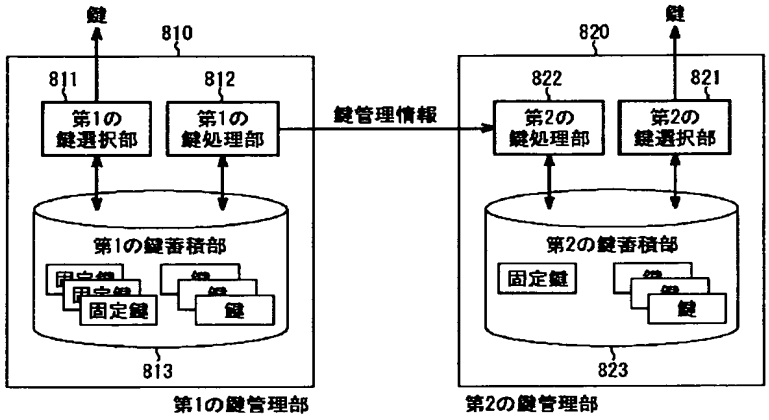
【図６】


12
放送事業者
121
122
番組情報
暗号化部
多重化部
鍵
123
第1の
鍵管理部
鍵管理情報
通信媒体
14
受信者
141
142
分離部
復号部
番組情報
143
鍵
第2の
鍵管理部
鍵管理情報
メタ情報
第2の
暗号化部
131
鍵
第3の
鍵管理部
132
13
メタ情報提供業者

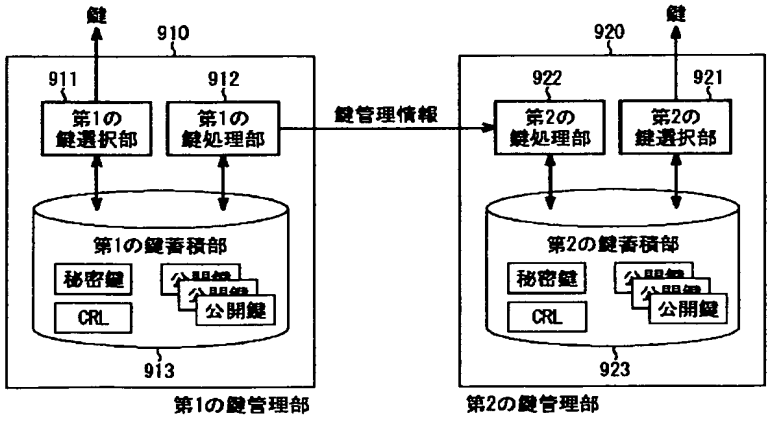
【図７】


ストレージ
70
71
72
番組情報
スクランブル部
多重化部
73
スクランブル鍵Ks
第1の暗号化部
74
ワーク鍵
契約情報
第2の暗号化部
鍵管理情報
75
第1の鍵管理部
放送事業者側の放送装置
80
81
82
分離部
デスクランブル部
番組情報
83
スクランブル鍵
第1の復号部
視聴判定部
85
84
ワーク鍵
第2の復号部
契約情報
鍵管理情報
第2の鍵管理部
86
受信者側の受信装置

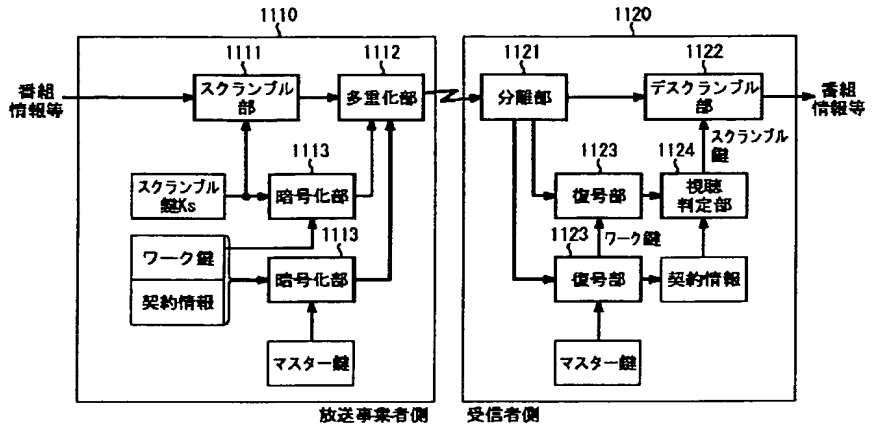
【図８】


鍵
810
811
812
第1の鍵選択部
第1の鍵処理部
鍵管理情報
第1の鍵蓄積部
固定鍵
鍵
813
第1の鍵管理部
鍵
820
822
821
第2の鍵処理部
第2の鍵選択部
第2の鍵蓄積部
固定鍵
鍵
823
第2の鍵管理部

【図９】


鍵
910
911
912
第1の鍵選択部
第1の鍵処理部
鍵管理情報
第1の鍵蓄積部
秘密鍵
CRL
公開鍵
913
第1の鍵管理部
鍵
920
922
921
第2の鍵処理部
第2の鍵選択部
第2の鍵蓄積部
秘密鍵
CRL
公開鍵
923
第2の鍵管理部

【図１１】



フロントページの続き

(51) Int. Cl.[7]	識別記号	F I		テーマコード（参考）
Ｈ０４Ｎ　7/167		Ｈ０４Ｎ	5/91	Ｌ
		Ｈ０４Ｌ	9/00	６０１Ｂ

Ｆターム(参考)　5C025 BA25 BA30 DA01 DA04 DA10
5C053 FA20 GB06 GB40 LA14
5C064 BA01 BB02 BC07 BC17 BC22
BC25 BD03 BD08 BD09 CA18
CB01 CB05 CC02
5J104 AA16 EA04 EA09 EA18 EA19
PA05

(54)【発明の名称】　デジタルコンテンツ処理装置、デジタル放送受信装置、デジタルコンテンツ処理システム、デジタル放送システム、デジタルコンテンツ処理方法、コンピュータ読み取り可能な記憶媒体及びコンピュータプログラム

【公報種別】特許法第１７条の２の規定による補正の掲載
【部門区分】第７部門第３区分
【発行日】平成16年12月2日(2004.12.2)

【公開番号】特開2003-244127(P2003-244127A)
【公開日】平成15年8月29日(2003.8.29)
【出願番号】特願2002-42133(P2002-42133)
【国際特許分類第７版】
ＨＯ４Ｌ　9/08
ＨＯ４Ｈ　1/00
ＨＯ４Ｎ　5/44
ＨＯ４Ｎ　5/765
ＨＯ４Ｎ　7/16
ＨＯ４Ｎ　7/167
【ＦＩ】
ＨＯ４Ｌ　9/00　６０１Ａ
ＨＯ４Ｈ　1/00　Ｆ
ＨＯ４Ｎ　5/44　Ａ
ＨＯ４Ｎ　7/16　Ａ
ＨＯ４Ｎ　7/167　Ｚ
ＨＯ４Ｎ　5/91　Ｌ
ＨＯ４Ｌ　9/00　６０１Ｂ

【手続補正書】
【提出日】平成15年12月11日(2003.12.11)
【手続補正１】
【補正対象書類名】明細書
【補正対象項目名】特許請求の範囲
【補正方法】変更
【補正の内容】
【特許請求の範囲】
【請求項１】
デジタルコンテンツまたは前記デジタルコンテンツに関するメタ情報を取り扱うデジタルコンテンツ処理装置であって、
前記デジタルコンテンツまたは前記メタ情報を制御するための第１の制御情報を保持し、入力される第２の制御情報によって前記保持している第１の制御情報を管理する管理手段と、
前記デジタルコンテンツまたは前記メタ情報の利用を前記第１の制御情報によって制御する制御手段とを有することを特徴とするデジタルコンテンツ処理装置。
【請求項２】
前記第１の制御情報は、共通鍵暗号方式における暗号化鍵であることを特徴とする請求項１に記載のデジタルコンテンツ処理装置。
【請求項３】
前記管理手段は、前記暗号化鍵を消去することによって前記第１の制御情報を管理することを特徴とする請求項２に記載のデジタルコンテンツ処理装置。
【請求項４】
前記管理手段は、前記暗号化鍵を更新することによって前記第１の制御情報を管理することを特徴とする請求項２に記載のデジタルコンテンツ処理装置。
【請求項５】
前記第１の制御情報は、公開鍵暗号方式における復号鍵であることを特徴とする請求項１

に記載のデジタルコンテンツ処理装置。
【請求項６】
前記管理手段は、前記公開鍵暗号方式における無効化リストによって前記第１の制御情報を管理することを特徴とする請求項５に記載のデジタルコンテンツ処理装置。
【請求項７】
前記第１の制御情報は、前記デジタルコンテンツまたは前記メタ情報に対応づけられていることを特徴とする請求項１～６の何れか１項に記載のデジタルコンテンツ処理装置。
【請求項８】
前記第１の制御情報は、前記デジタルコンテンツまたは前記メタ情報の配信者に対応づけられていることを特徴とする請求項１～６の何れか１項に記載のデジタルコンテンツ処理装置。
【請求項９】
前記第１の制御情報を管理する管理手段は、不正操作の困難な媒体で実現されていることを特徴とする請求項１～８の何れか１項に記載のデジタルコンテンツ処理装置。
【請求項１０】
前記デジタルコンテンツまたは前記メタ情報を記憶しておく記憶手段を有することを特徴とする請求項１～９の何れか１項に記載のデジタルコンテンツ処理装置。
【請求項１１】
前記デジタルコンテンツまたは前記メタ情報を受信する受信手段を有することを特徴とする請求項１～１０の何れか１項に記載のデジタルコンテンツ処理装置。
【請求項１２】
前記請求項１～１１の何れか１項に記載のデジタルコンテンツ処理装置を用いて、前記デジタルコンテンツである放送コンテンツを取り扱うことを特徴とするデジタル放送受信装置。
【請求項１３】
前記請求項１～１１の何れか１項に記載のデジタルコンテンツ処理装置を有することを特徴とするデジタルコンテンツ処理システム。
【請求項１４】
前記請求項１～１１の何れか１項に記載のデジタルコンテンツ処理装置を有することを特徴とするデジタル放送システム。
【請求項１５】
デジタルコンテンツ及び前記デジタルコンテンツに関するメタ情報を取り扱うデジタルコンテンツ処理方法であって、
前記デジタルコンテンツまたは前記メタ情報を制御するための第１の制御情報を媒体に保持し、入力される第２の制御情報によって前記保持している第１の制御情報を管理する管理工程と、
前記デジタルコンテンツまたは前記メタ情報の利用を前記第１の制御情報によって制御する制御工程とを有することを特徴とするデジタルコンテンツ処理方法。
【請求項１６】
前記第１の制御情報は、共通鍵暗号方式における暗号化鍵であることを特徴とする請求項１５に記載のデジタルコンテンツ処理方法。
【請求項１７】
前記管理工程は、前記暗号化鍵を消去することによって前記第１の制御情報を管理することを特徴とする請求項１６に記載のデジタルコンテンツ処理方法。
【請求項１８】
前記管理工程は、前記暗号化鍵を更新することによって前記第１の制御情報を管理することを特徴とする請求項１６に記載のデジタルコンテンツ処理方法。
【請求項１９】
前記第１の制御情報は、公開鍵暗号方式における復号鍵であることを特徴とする請求項１５に記載のデジタルコンテンツ処理方法。

【請求項２０】
前記管理工程は、前記公開鍵暗号方式における無効化リストによって前記第１の制御情報を管理することを特徴とする請求項１９に記載のデジタルコンテンツ処理方法。
【請求項２１】
前記第１の制御情報は、前記デジタルコンテンツまたは前記メタ情報に対応づけられていることを特徴とする請求項１５～２０の何れか１項に記載のデジタルコンテンツ処理方法。
【請求項２２】
前記第１の制御情報は、前記デジタルコンテンツまたは前記メタ情報の配信者に対応づけられていることを特徴とする請求項１５～２０の何れか１項に記載のデジタルコンテンツ処理方法。
【請求項２３】
前記請求項１５～２２の何れか１項に記載のデジタルコンテンツ処理方法をコンピュータに実行させるためのプログラムを記録したことを特徴とするコンピュータ読み取り可能な記憶媒体。
【請求項２４】
前記請求項１５～２２の何れか１項に記載のデジタルコンテンツ処理方法をコンピュータに実行させることを特徴とするコンピュータプログラム。
【手続補正２】
【補正対象書類名】明細書
【補正対象項目名】００２４
【補正方法】変更
【補正の内容】
【００２４】
【課題を解決するための手段】
本発明のデジタルコンテンツ処理装置は、デジタルコンテンツまたは前記デジタルコンテンツに関するメタ情報を取り扱うデジタルコンテンツ処理装置であって、前記デジタルコンテンツまたは前記メタ情報を制御するための第１の制御情報を保持し、入力される第２の制御情報によって前記保持している第１の制御情報を管理する管理手段と、前記デジタルコンテンツまたは前記メタ情報の利用を前記第１の制御情報によって制御する制御手段とを有することを特徴としている。
また、本発明の他の特徴とするところは、前記第１の制御情報は、共通鍵暗号方式における暗号化鍵であることを特徴としている。
また、本発明のその他の特徴とするところは、前記管理手段は、前記暗号化鍵を消去することによって前記第１の制御情報を管理することを特徴としている。
また、本発明のその他の特徴とするところは、前記管理手段は、前記暗号化鍵を更新することによって前記第１の制御情報を管理することを特徴としている。
また、本発明のその他の特徴とするところは、前記第１の制御情報は、公開鍵暗号方式における復号鍵であることを特徴としている。
また、本発明のその他の特徴とするところは、前記管理手段は、前記公開鍵暗号方式における無効化リストによって前記第１の制御情報を管理することを特徴としている。
また、本発明のその他の特徴とするところは、前記第１の制御情報は、前記デジタルコンテンツまたは前記メタ情報に対応づけられていることを特徴としている。
また、本発明のその他の特徴とするところは、前記第１の制御情報は、前記デジタルコンテンツまたは前記メタ情報の配信者に対応づけられていることを特徴としている。
また、本発明のその他の特徴とするところは、前記第１の制御情報を管理する管理手段は、不正操作の困難な媒体で実現されていることを特徴としている。
また、本発明のその他の特徴とするところは、前記デジタルコンテンツまたは前記メタ情報を記憶しておく記憶手段を有することを特徴としている。
また、本発明のその他の特徴とするところは、前記デジタルコンテンツまたは前記メタ情

報を受信する受信手段を有することを特徴としている。
【手続補正３】
【補正対象書類名】明細書
【補正対象項目名】００２９
【補正方法】変更
【補正の内容】
【００２９】
本発明の記憶媒体は、前記の何れかに記載のデジタルコンテンツ処理方法をコンピュータに実行させるためのプログラムを記録したことを特徴としている。